

### **REMARKS**

In response to the final Office Action mailed May 6, 2004, and in view of the Request for Continued Examination (RCE) submitted on September 7, 2004 (or alternately the Supplemental RCE submitted herewith), Applicant respectfully requests reconsideration. Claims 1-27 and 29-32 were previously pending in this application. Claims 1, 2, 6-8, 15, 21 and 24 are amended herein. Claim 5 is canceled. Accordingly, claims 1-4, 6-27 and 29-33 are pending in this application, of which claims 1, 15 and 21 are independent claims.

#### **I. Rejection Under 35 U.S.C. §103**

In the Office Action, all of the claims (including independent claims 1, 15 and 21) are rejected under 35 U.S.C. 103(a) as purportedly being obvious over Ericson (U.S. Patent No. 6,061,753) in view of Yu (U.S. Patent No. 4,919,545). This rejection is respectfully traversed.

The Office Action relies on Yu to purportedly provide “authenticating the request at the storage system to authenticate the device issuing the request,” which the Office Action concedes as missing in the Ericson reference. Each of the independent claims has been amended to distinguish over the authentication procedures of Yu.

Yu discloses an authentication method wherein an encryption key to encrypt a signature used to authenticate a capability request is generated and maintained at an execution node where an object being requested is located (i.e., not at a node requesting access to the object). The node then transmits the encryption key to an invocation node requesting a capability. In particular, column 6, line 67 – column 7, line 28 state in relevant part:

A signature 44 is used to protect the capability. The signature 44 is obtained as shown in FIG. 5 by encrypting the object identifying the object identifier field 40 and the access right field 42 with an encryption key 46 in an encryption step 48. The encryption key 46 is secured in the node operating system of the node where the object of [sic] located...A process requiring access to the object is located at an invocation node 52. The execution node 50 first grants permission to access the object by generating a capability and a signature, and transmitting the capability and the signature to the invocation node 52.

The signature, therefore, is encrypted with an encryption key having its origin at the execution node. Yu is completely silent with respect to encrypting a signature with an encryption key provided by the invocation node.

Claim 1, as amended, recites a data management method for managing access to a plurality of volumes of a storage system by at least two devices coupled to the storage system through a network. The method comprising steps of receiving, over the network at the storage system, encryption information provided by each of the at least two devices, transferring an expected access key between the storage system and each of the at least two devices, the expected access key encrypted via the respective encryption information, receiving over the network at the storage system a request from one of the at least two devices for access to at least one of the plurality of volumes of the storage system, the request identifying the at least one of the plurality of volumes in the storage system, and including a request access key, and selectively servicing, at the storage system, the request responsive to configuration data indicating that the one of the at least two devices is authorized to access the at least one of the plurality of volumes, wherein the step of selectively servicing comprises a step of verifying that the represented source of the request is the one of the at least two devices that issued the request based, at least in part, on a comparison between the requested access key and the expected access key.

Nowhere does the combination of Ericson and Yu disclose or suggest “receiving, over the network at the storage system, encryption information provided by each of the at least two devices” wherein an expected access key transferred between a device and a storage system is “encrypted via the encryption information,” as recited in claim 1. Therefore, claim 1 patentably distinguishes over the combination and is in allowable condition.

Claims 2-4 and 6-14 depend from claim 1 and are allowable for at least the same reason.

Claim 15, as amended, recites a first data structure having configuration information that includes “an access key previously transferred between each of the plurality of devices and the storage system, the access key encrypted with encryption information initially provided by a respective one of the plurality of devices.” Nowhere does the combination of Ericson and Yu disclose or suggest an access key encrypted via encryption information having one of the plurality of devices as the initial source. Therefore, claim 15 patentably distinguishes over the combination and is in allowable condition.

Claims 16-20 depend from claim 15 and are allowable for at least the same reason.

Claim 21, as amended, recites a configuration table “to store an expected access key for each of the plurality of devices, the access key transferred between a respective one of the plurality of devices and the storage system and encrypted for the transfer using encryption information initially provided by the respective one of the plurality of devices.” Nowhere does the combination of Ericson and Yu disclose or suggest a configuration table to store an access key encrypted by information having a device seeking access as the source of the information. Therefore, claim 21 patentably distinguishes over the combination and is in allowable condition.

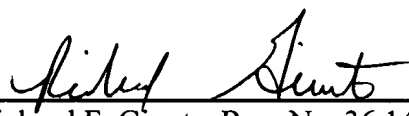
Claims 22-32 depend from claim 21 and are allowable for at least the same reason.

### CONCLUSION

In view of the foregoing amendments and remarks, this application should now be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below to discuss any outstanding issues relating to the allowability of the application.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Respectfully submitted,  
*Steven M. Blumenau et al., Applicant*

By:   
Richard F. Giunta, Reg. No. 36,149  
Wolf, Greenfield & Sacks, P.C.  
600 Atlantic Avenue  
Boston, Massachusetts 02210-2211  
Telephone: (617) 720-3500

Docket No.E0295.70066US00  
Date: November 8, 2004  
xNDD